09/757963

C of C

+

0801/PTO
Rev. 10/95

U.S. Department of Commerce
Patent and Trademark Office

TRANSMITTAL FORM

(to be used for all correspondence during pendency of filed application)

Patent Number	6,957,348
Issue Date	October 18, 2005
First Named Inventor	John S. Flowers
Group Art Unit Number	2131
Examiner Name	Aravind K. Moorthy
Total Number of Pages in This Submission	13
Attorney Docket Number	23327-06896

ENCLOSURES *(check all that apply)*

- □ Fee Transmittal Form (in duplicate)
  - □ Check Enclosed
- ☒ Return Receipt Postcard
- □ Response to Notice to File Missing Parts
- □ Assignment & Recordation Cover Sheet
- □ Declaration
- □ Power of Attorney
- □ Application Data Sheet
- □ Information Disclosure Statement & PTO/SB/08A
  - □ Copies of IDS Cited References
- □ Request for Corrected Filing Receipt
- □ Request for Correction of Recorded Assignment
- □ Amendment: [ ] Page(s)
  - □ After Final
- □ Status Request
- □ Revocation and Substitute Power of Attorney
- □ Issue Fee Transmittal (in duplicate)
- □ Letter to Chief Draftsperson
- □ Formal Drawing(s):
  [ ] Sheet(s) of Figure(s) [ ]
- □ Appeal Communication to Board of Appeals and Interferences
- □ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- □ Certified Copy of Priority Document(s)
- □ After Allowance Communication to Group
- ☒ Request for Certificate of Correction
- ☒ a copy of an Amendment filed on 09/03/04
- □ ____
- □ ____
- □ ____
- □ ____

REMARKS:

SIGNATURE OF ATTORNEY OR AGENT

Signature:	Dorian Cartwright		
Attorney/Reg. No.:	Dorian Cartwright, Reg. No. 53,853	Dated:	11/15/05

CERTIFICATE OF MAILING

I hereby certify that this correspondence, including the enclosures identified above, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.

Signature:	Dorian Cartwright		
Typed or Printed Name:	Dorian Cartwright	Dated:	11/15/05
Express Mail Mailing Number (*optional*):			

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S):	John S. Flowers *et al.*
PATENT NO.:	6,957,348
ISSUE DATE:	October 18, 2005
SERIAL NO.:	09/757,963
FILING DATE:	January 10, 2001
TITLE:	INTEROPERABILITY OF VULNERABILITY AND INTRUSION DETECTION SYSTEMS
EXAMINER:	Aravind K. Moorthy
GROUP ART UNIT:	2131
ATTY. DKT. NO.:	23327-06896

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: DECISION AND CERTIFICATE OF CORRECTION BRANCH OF THE PATENT ISSUE DIVISION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Dated: 11/15/05 By: Dorian Cartwright

Dorian Cartwright, Reg. No. 53,853

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

ATTENTION: DECISION AND CERTIFICATE OF CORRECTION
BRANCH OF THE PATENT ISSUE DIVISION

REQUEST FOR CERTIFICATE OF CORRECTION

SIR:

The following errors, as more fully described below, appear in this patent.

☒ The Applicant submits that no fee is due for correction of the errors made by the Patent and Trademark Office.

Attached hereto are duplicate Forms PTO-1050, with at least one copy that is suitable for printing. Also enclosed is a copy of an Amendment filed on September 3, 2004 showing the text of the allowed claims.

Applicant kindly requests the following changes:

Claim 2, at column 14, line 1, please change "form" to "from";

Claim 7, at column 14, line 25, please change "application" to "applications";

Claim 8, at column 14, line 27, please change "communications" to "communication"; and

Claim 19, at column 15, line 12, please change "exploitation" to "exploitations."

Please send the Certificate to:
DORIAN CARTWRIGHT
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041

RESPECTFULLY SUBMITTED,
John S. Flowers *et al.*

Date: 11/15/2005

By: Dorian Cartwright

Dorian Cartwright, Applicant's Attorney
Registration No. 53,853
FENWICK & WEST LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7247
Fax: (650) 938-5200

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.: 6,957,348 B1

DATED: October 18, 2005

INVENTORS: John S. Flowers *et al.*

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Claim 2, at column 14, line 1, please change “form” to “from”;

Claim 7, at column 14, line 25, plèase change “application” to “applications”;

Claim 8, at column 14, line 27, please change “communications” to “communication”; and

Claim 19, at column 15, line 12, please change “exploitation” to “exploitations.”

MAILING ADDRESS OF SENDER:
Dorian Cartwright
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041

PATENT NO. 6,957,348 B1

No, of add’l copies
@50¢ per page
⇨ ________

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.: 6,957,348 B1

DATED: October 18, 2005

INVENTORS: John S. Flowers *et al.*

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Claim 2, at column 14, line 1, please change “form” to “from”;

Claim 7, at column 14, line 25, please change “application” to “applications”;

Claim 8, at column 14, line 27, please change “communications” to “communication”; and

Claim 19, at column 15, line 12, please change “exploitation” to “exploitations.”

MAILING ADDRESS OF SENDER:
Dorian Cartwright
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041

PATENT NO. 6,957,348 B1

No, of add’l copies
@50¢ per page
⇨ ________

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: John S. Flowers *et al.*

SERIAL NO.: 09/757,963

FILING DATE: January 10, 2001

TITLE: INTEROPERABILITY OF VULNERABILITY AND INTRUSION DETECTION SYSTEMS

EXAMINER: Aravind K. Moorthy

GROUP ART UNIT: 2131

ATTY. DKT. NO.: 23327-06896

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Dated: September 3, 2004 By: Dorian Cartwright

Dorian Cartwright, Reg. No. 53,853

MAIL STOP ISSUE FEE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT E UNDER §1.312

SIR:

In response to the *Notice of Allowability* with an *Examiner's Amendment* dated August 25, 2004 (paper no. 22), which was included with a *Notice of Allowance and and Fee(s) Due* seting a deadline of November 26, 2004 to pay the issue fee and the publication fee, kindly amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 7 of this paper.

In The Claims

The listing of claims will replace all prior versions, and listings, of claims in the application. In the listing, claim 29 is hereby amended.

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Previously Presented) A computer-implemented system for protecting a network, comprising:

a vulnerability detection system (VDS) for gathering information about the network to determine vulnerabilities of a host from a plurality of hosts on the network; and

an intrusion detection system (IDS), cooperative with the VDS, for examining network traffic responsive to the vulnerabilities of the host from the plurality of hosts as determined by the VDS to detect traffic indicative of malicious activity.

6. (Previously Presented) The system of claim 5, wherein the VDS is adapted to gather information about the network by sending data to the plurality of hosts and receiving responsive data from the plurality of hosts.

7. (Previously Presented) The system of claim 5, wherein the VDS is adapted to gather information automatically provided by the plurality of hosts.

8. (Previously Presented) The system of claim 5, further comprising:

a vulnerabilities rules database, in communication with the VDS, for storing rules describing vulnerabilities of the plurality of hosts,

wherein the VDS is adapted to analyze the gathered information with the rules to determine the vulnerabilities of the plurality of hosts.

9. (Previously Presented) The system of claim 8, wherein the VDS is adapted to analyze the gathered information with the rules to identify operating systems on the plurality of hosts and determine the vulnerabilities responsive to the respective operating systems.

10. (Previously Presented) The system of claim 8, wherein the VDS is adapted to analyze the gathered information with the rules to identify open ports on the plurality of hosts and determine the vulnerabilities based on the open ports.

11. (Previously Presented) The system of claim 8, wherein the VDS is adapted to analyze the gathered information with the rules to identify applications executing on the plurality of hosts and determine the vulnerabilities based on the applications.

12. (Original) The system of claim 5, further comprising:

an intrusion rules database, in communication with the IDS, for storing rules describing malicious activity,

wherein the IDS is adapted to analyze the network traffic with the rules to detect network traffic indicative of exploitations of the determined vulnerabilities.

13. (Original) The system of claim 5, wherein the IDS is adapted to detect traffic indicative of exploitations of only the determined vulnerabilities.

14. (Cancelled)

15. (Original) The system of claim 5, wherein the VDS is adapted to update the determined vulnerabilities, and wherein the IDS is adapted to detect traffic indicative of malicious activity in response to the update.

16. (Original) The system of claim 15, wherein the VDS is adapted to update the determined vulnerabilities in response to a change in the network.

17. (Previously Presented) A computer-implemented method for protecting a network, comprising:

gathering information about the network to determine vulnerabilities of a host from a plurality of hosts on the network; and

cooperative with the step of gathering information, examining network traffic responsive to the determined vulnerabilities of the host from the plurality of hosts to detect network traffic indicative of malicious activity.

18. (Previously Presented) The method of claim 17, wherein gathering information comprises sending data to plurality of hosts on the network and receiving responsive data from the plurality of hosts.

19. (Previously Presented) The method of claim 17, wherein gathering information comprises receiving data automatically provided by the plurality of hosts on the network.

20. (Previously Presented) The method of claim 17, further comprising:

storing rules to describe vulnerabilities of the plurality of hosts,

wherein determining vulnerabilities includes analyzing the gathered information with the rules.

21. (Previously Presented) The method of claim 20, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify operating systems on the plurality of hosts.

22. (Previously Presented) The method of claim 20, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify open ports on the plurality of hosts.

23. (Previously Presented) The method of claim 20, wherein determining vulnerabilities comprises comparing the gathered information against the rules to identify applications on the plurality of hosts.

24. (Original) The method of claim 17, further comprising:

storing rules describing malicious activity,

wherein detecting network traffic indicative of malicious activity comprises analyzing the network traffic with the rules to detect traffic indicative of exploitations of the determined vulnerabilities.

25. (Original) The method of claim 17, wherein examining network traffic consists of detecting traffic indicative of exploitations of only the determined vulnerabilities.

26. (Cancelled)

27. (Previously Presented) The method of claim 17, further comprising:

updating the determined vulnerabilities and detecting traffic indicative of malicious activity in response to the update.

28. (Original) The method of claim 27, wherein the updating is responsive to a change in the network.

29. (Currently Amended) A computer program product, comprising:

a computer-readable medium having computer program logic embodied therein for protecting a network, the computer program logic:

gathering information about the network to determine vulnerabilities of a host from a plurality of hosts on the network; and

cooperative with the step of gathering information, examining network traffic responsive to the determined vulnerabilities of the host from the plurality of hosts to detect network traffic indicative of malicious activity.

30. (Previously Presented) The computer program product of claim 29, wherein gathering information comprises sending data to plurality of hosts on the network and receiving responsive data from the plurality of hosts.

31. (Previously Presented) The computer program product of claim 29, wherein gathering information comprises receiving data automatically provided by the plurality of hosts on the network.

32. (Previously Presented) The computer program product of claim 29, further comprising:

storing rules to describe vulnerabilities of the plurality of hosts,

wherein determining vulnerabilities includes analyzing the gathered information with the rules.

33. (Previously Presented) The computer program product of claim 32, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify operating systems on the plurality of hosts.

34. (Previously Presented) The computer program product of claim 32, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify open ports on the plurality of hosts.

35. (Previously Presented) The computer program product of claim 32, wherein determining vulnerabilities comprises comparing the gathered information against the rules to identify applications on the plurality of hosts.

36. (Original) The computer program product of claim 29, further comprising:

storing rules describing malicious activity,

wherein detecting network traffic indicative of malicious activity comprises analyzing the network traffic with the rules to detect traffic indicative of exploitations of the determined vulnerabilities.

37. (Original) The computer program product of claim 29, wherein examining network traffic consists of detecting traffic indicative of exploitations of only the verified vulnerabilities.

38. (Cancelled)

39. (Previously Presented) The computer program product of claim 29, further comprising:

updating the determined vulnerabilities; and

detecting traffic indicative of malicious activity in response to the update.

40. (Previously Presented) The computer program product of claim 39, wherein the updating is responsive to a change in the network.

REMARKS

Claims 5-13, 15-25, 27-37, 39 and 40 were allowed by the Examiner in the *Notice of Allowability*. Applicants herein amend claim 29. No new matter is added by the claim amendment. Applicants now request that the amendment to the claim made after allowance be entered pursuant to CFR §1.312 and MPEP §714.16.

Applicants thank Examiner for examination an allowance of the claims pending in this application. Applicants have amended claim 29 merely to add the word "a" which was erroneously omitted from the *Examiner's Amendment*. Applicants submit that such amendment does not change the scope of the allowed claims.

Applicants respectfully request entry of above amendment. Also, Applicants invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

RESPECTFULLY SUBMITTED,
John S. Flowers *et al.*

Date: September 3, 2004

By: Dorian Cartwright

Dorian Cartwright, Applicant's Attorney
Registration No. 53,853
FENWICK & WEST LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7247
Fax: (650) 938-5200